CLAIMS

What is claimed is:

1. A system, comprising:

a logic configured to perform one or more of, cryptographic key maintenance, and cryptographic key migration for a trusted platform to which the logic may be bound in a one-to-one manner; and

an interface configured to facilitate operably connecting the system to the trusted platform.

2. The system of claim 1, where the cryptographic key maintenance and the cryptographic key migration performed by the logic comply with the Trusted Computing Group (TCG) specification version 1.1b.

3. The system of claim 1, where the logic comprises an application specific integrated circuit (ASIC).

4. The system of claim 1, where the logic comprises a microprocessor operably connected to a non-volatile memory.

5. The system of claim 1, where the logic and the interface comprise part of a USB token.

6. The system of claim 1, where the interface is configured to facilitate operably connecting the system to the trusted platform by one or more of, a Universal Serial Bus interface, a Small Computer Systems Interface interface, a Peripheral Component Interconnect interface, a PCI Express (PCIE) interface, a 1394 interface, an Industrial Standard Architecture interface, an Extended Industrial Standard Architecture interface, a wireless connection, and a microchannel interface.

7. The system of claim 1, where performing cryptographic key maintenance includes cloning the trusted platform with the cooperation of a manufacturer of the trusted platform and an owner of the trusted platform.

8. The system of claim 7, where performing cryptographic key maintenance includes having the manufacturer of the trusted platform act as an intermediary and migrating a non-migratable storage root key from a root of a key storage hierarchy associated with a trusted platform module associated with the trusted platform.

9. The system of claim 1, where performing cryptographic key migration includes logically attaching a trusted platform module migratable key data structure associated with a first protected storage tree to a second protected storage tree.

10. The system of claim 1, where the logic is configured to store one or more of, a copy of a storage root key, a binding data that facilitates binding the logic to the trusted platform in a one-to-one binding, a processor executable set of instructions that facilitate the trusted platform determining that the trusted platform is interfacing with the logic instead of a trusted platform module, and a processor readable set of data that facilitates the trusted platform determining that the trusted platform is interfacing with the logic instead of a trusted platform module.

11. The system of claim 1, where the logic is configured to facilitate substantially instantaneously restoring a trusted platform module.

12. The system of claim 1, where the logic is configured to decrypt one or more of, a key, and a piece of data encrypted by a trusted platform module.

13. The system of claim 1, where the logic is configured to execute processor executable instructions associated with the logic while preventing execution of processor executable instructions not associated with the logic.

14. The system of claim 1, where the logic is configured to read processor readable data associated with the logic while preventing a second logic from reading the processor readable data associated with the logic.

15. The system of claim 1, where the logic is configured to detect whether there is a functional trusted platform module associated with the trusted platform.

16. The system of claim 1, where the logic is configured to prevent creation of a new cryptographic key by the system and to prevent performance of an attestation service by the logic.

17. The system of claim 1, where binding the logic to the trusted platform in a one-to-one manner includes producing an optimal asymmetric encryption padding (OEAP) binary large object to facilitate copying a storage root key stored in a trusted platform module associated with the trusted platform.

18. The system of claim 1, where the logic is configured to perform a finite number of cryptographic key maintenance or migration operations.

19. A system, comprising:

a logic configured to perform one or more of, cryptographic key maintenance and cryptographic key migration for a trusted platform to which the logic may be bound in a one-to-one manner,

where performing cryptographic key maintenance includes one or more of, cloning the trusted platform with the cooperation of a manufacturer of the trusted platform and an owner of the trusted platform, and having the manufacturer of the trusted platform act as an intermediary and migrating a non-migratable storage root key from the root of a key storage hierarchy associated with a trusted platform module associated with the trusted platform,

and where performing cryptographic key migration includes logically attaching a trusted platform module migratable key data structure associated with a first protected storage tree to a second protected storage tree;

the logic being further configured to perform one or more of, storing a copy of a storage root key, storing a binding data that facilitates binding the logic to the trusted

platform in a one-to-one binding, storing a processor executable set of instructions that facilitate the trusted platform determining that the trusted platform is interfacing with the logic instead of a trusted platform module, storing a processor readable set of data that facilitates the trusted platform determining that the trusted platform is interfacing with the logic instead of a trusted platform module, facilitating substantially instantaneously restoring a trusted platform module, decrypting a key encrypted by the logic, executing a first set of processor executable instructions associated with the logic while preventing execution of a second set of processor executable instructions not associated with the logic, reading a set of processor readable data associated with the logic while preventing another logic from reading the set of processor readable data associated with the logic, and detecting whether there is a functional trusted platform module associated with the trusted platform,

the logic being further configured to prevent creation of a new cryptographic key by the system, to prevent the performance of an attestation service by the system, and to prevent performance of an authentication service by the system; and

an interface configured to facilitate operably connecting the system to the trusted platform.

20. A subordinate trusted platform module, comprising:

a restore logic configured to perform one or more of, cryptographic key maintenance, and cryptographic key migration for a trusted platform to which the subordinate trusted platform module may be bound in a one-to-one manner;

a memory operably connected to the restore logic, the memory being configured to store one or more of, a storage root key, and a set of processor executable instructions associated with performing a cryptographic key maintenance operation;

a processor operably connected to one or more of, the restore logic, and the memory, the processor being configured to perform one or more of, a cryptographic key maintenance operation, and an interface action associated with operably connecting the subordinate trusted platform module to a trusted platform; and

an interface configured to facilitate operably connecting the subordinate trusted platform module to a trusted platform.

21. The subordinate trusted platform module of claim 20, where the subordinate trusted platform module comprises a Universal Serial Bus token.

22. The subordinate trusted platform module of claim 20, where a cryptographic key maintenance operation includes one or more of, cloning the trusted platform with the cooperation of a manufacturer of the trusted platform and an owner of the trusted platform, and having the manufacturer of the trusted platform act as an intermediary and migrating a non-migratable storage root key from a root of a key storage hierarchy associated with a trusted platform module associated with the trusted platform.

23. The subordinate trusted platform module of claim 20, where the processor is further configured to perform a cryptographic key migration operation that includes logically attaching a trusted platform module migratable key data structure associated with a first protected storage tree to a second protected storage tree.

24. The subordinate trusted platform module of claim 20, where the processor is configured to perform one or more of, automatically executing processor executable instructions when the subordinate trusted platform module is operably connected to the trusted platform, and to manage a key hierarchy associated with the trusted platform.

25. A method for securely backing up a cryptographic key stored in a trusted platform module associated with a trusted platform, comprising:

determining whether to perform a cryptographic key maintenance operation;

upon determining to perform a cryptographic key maintenance operation, establishing an operable connection between a subordinate trusted platform module and the trusted platform;

requesting that the subordinate trusted platform module perform the cryptographic key maintenance operation;

controlling the subordinate trusted platform module to determine whether a trusted platform module is associated with the trusted platform;

upon determining that a trusted platform module is associated with the trusted platform, controlling the subordinate trusted platform module to interrogate the trusted platform to determine whether the trusted platform has previously had the cryptographic key stored in the trusted platform module backed up; and

upon determining that the cryptographic key stored in the trusted platform module has not been previously backed up, performing the cryptographic key maintenance operation to copy the cryptographic key stored in the trusted platform module to the subordinate trusted platform module.

26. The method of claim 25, where the subordinate trusted platform module supports one or more functionalities defined in a TCG specification.

27. The method of claim 26, where the one or more functionalities include TPM_LoadManualMaintPub, and TPM_ReadManualMaintPub.

28. The method of claim 26, where establishing an operable connection between the subordinate trusted platform module and the trusted platform includes inserting a Universal Serial Bus token into a Universal Serial Bus interface associated with the trusted platform.

29. A computerized method for securely backing up, in a subordinate trusted platform module, a storage root key stored in a trusted platform module, the method comprising:

establishing an operable connection between the subordinate trusted platform module and the trusted platform module;

receiving a request to back up the storage root key;

determining whether the storage root key has been previously backed up;

upon determining that the storage root key has not been previously backed up, copying the storage root key to the subordinate trusted platform module; and

disestablishing the operable connection between the subordinate trusted platform module and the trusted platform module.

30. The method of claim 29, where establishing the operable connection includes inserting the subordinate trusted platform module into a Universal Serial Bus interface associated with the trusted platform associated with the trusted platform module.

31. The method of claim 29, including establishing a one-to-one binding between the subordinate trusted platform module and the trusted platform module.

32. A method for employing a cryptographic key stored in a subordinate trusted platform module, comprising:

establishing an operable connection between the subordinate trusted platform module and a trusted platform associated with a key hierarchy produced by a trusted platform module;

validating that the trusted platform can interact with the subordinate trusted platform module and can employ the cryptographic key;

generating a request to employ the cryptographic key;

associating the cryptographic key with the key hierarchy;

decrypting an encrypted item in the key hierarchy using the cryptographic key;

controlling the subordinate trusted platform module to be reconfigured to indicate that the subordinate trusted platform module performed a requested maintenance operation; and

disestablishing the operable connection between the subordinate trusted platform module and the trusted platform.

33. The method of claim 32, where establishing the operable connection between the subordinate trusted platform module and the trusted platform includes inserting the subordinate trusted platform module into a Universal Serial Bus interface operably connected to the trusted platform.

34. The method of claim 32, where validating that the trusted platform can interact with the subordinate trusted platform module includes determining that the subordinate trusted platform module has a one-to-one binding with the trusted platform.

35. The method of claim 32, where associating the cryptographic key with the key hierarchy includes logically connecting the cryptographic key to a root of the key hierarchy.

36. The method of claim 32, where controlling the subordinate trusted platform module to be reconfigured to indicate that the subordinate trusted platform module performed the requested maintenance operation includes causing the subordinate trusted platform module to be disabled from performing a subsequent maintenance operation.

37. The method of claim 32, where disestablishing the operable connection between the subordinate trusted platform module and the trusted platform includes removing the subordinate trusted platform module from a Universal Serial Bus interface operably connected to the trusted platform and breaking a one-to-one binding between the subordinate trusted platform module and the trusted platform.

38. A method for providing a storage root key stored in a subordinate trusted platform module to a trusted platform, comprising:

establishing an operable connection between the subordinate trusted platform module and the trusted platform;

validating that the subordinate trusted platform module can interact with the trusted platform;

determining whether a trusted platform module associated with the trusted platform is functional;

upon determining that the trusted platform module is not functional, providing the storage root key to the trusted platform;

reconfiguring the subordinate trusted platform module to indicate that the storage root key has been provided to the trusted platform; and

disestablishing the operable connection between the subordinate trusted platform module and the trusted platform.

39. The method of claim 38, where validating that the subordinate trusted platform module can interact with the trusted platform includes determining the existence of a one-to-one binding between the subordinate trusted platform module and the trusted platform.

40. The method of claim 38, where reconfiguring the subordinate trusted platform module includes disabling the subordinate trusted platform module from subsequently providing the storage root key.

41. A method for decrypting an item encrypted by a failed trusted platform module, comprising:

associating a subordinate trusted platform module that has been bound in a one-to-one manner with the failed trusted platform module with a trusted platform associated with the failed trusted platform module;

determining that the failed trusted platform module is not operational; and

decrypting the item using a copy of a storage root key stored in the subordinate trusted platform module, where the copy of the storage root key came from the failed trusted platform module.

42. A computer-readable medium storing processor executable instructions operable to perform a computerized method for securely backing up in a subordinate trusted platform module a storage root key stored in a trusted platform module, the method comprising:

receiving a request to back up the storage root key;

determining whether the storage root key has been previously backed up;

upon determining that the storage root key has not been previously backed up, copying the storage root key to the subordinate trusted platform module; and

establishing a one-to-one binding between the subordinate trusted platform module and the trusted platform module.

43. A computer-readable medium storing processor executable instructions operable to perform a method for providing a storage root key stored in a subordinate trusted platform module to a trusted platform, the method comprising:

validating that the subordinate trusted platform module can interact with the trusted platform;

determining whether a trusted platform module associated with the trusted platform is functional;

upon determining that the trusted platform module is not functional, providing the storage root key to the trusted platform; and

reconfiguring the subordinate trusted platform module to indicate that the storage root key has been provided to the trusted platform, where reconfiguring the subordinate trusted platform module includes disabling the subordinate trusted platform module from subsequently providing the storage root key.

44. A system, comprising:

means for performing one or more of, cryptographic key maintenance, and cryptographic key migration for a trusted platform;

means for operably connecting the system to the trusted platform; and

means for determining whether to perform one or more of, cryptographic key maintenance, and cryptographic key migration for the trusted platform.

45. A system, comprising:

an electronic apparatus configured with a trusted platform module; and

an interface operably connected to the electronic apparatus, the interface configured to facilitate operably, detachably connecting a subordinate trusted platform module to the electronic apparatus.

46. The system of claim 45, where the electronic apparatus comprises one of, a computer, a printer, a cellular telephone, and a digital camera.

47. In a computer system having a graphical user interface comprising a display and a selection device, a method of providing and selecting from a set of data entries on the display, the method comprising:

retrieving a set of data entries, where a data entry represents one or more of, a cryptographic key maintenance operation, and a cryptographic key migration operation;

displaying the set of data entries on the display;

receiving a data entry selection signal indicative of the selection device selecting a selected data entry; and

in response to the data entry selection signal, initiating one or more of, a cryptographic key maintenance operation, and a cryptographic key migration operation associated with the selected data entry.